July 1993/Number 2-93

security awareness bulletin

Inside:

Treaty Inspections and Security

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication **Unlimited reproduction authorized**

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Security Education and Awareness Team, 8000 Jefferson Davis Hwy, Bldg 33E, Richmond VA 23297-5091; (804) 279-5314, DSN 695-5314. Fax: (804) 279-5239 or DSN 695-5239. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310, (703) 695-8920, DSN 225-8920;
POC Jim McElroy

Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350 (202) 433-8858, DSN 288-8858;
POC Sue Jones

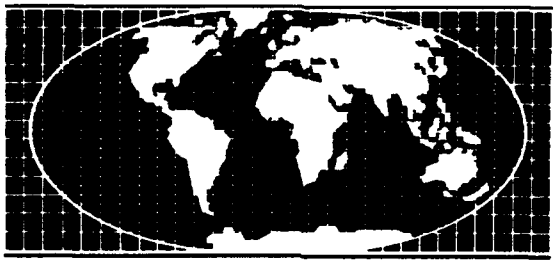
Air Force: Headquarters AFSPA/SPIB, 8201 H St SE, Kirtland AFB, NM 87117-5664, DSN 246-4787;
POC Ken Saxon

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria VA 22314-1651

DISP contractors: Cognizant Security Office

Other government agencies: Headquarters security education office

Arms Control Inspections and Industrial Security



by John T. Elliff
Director, Defense Security Programs
Office of the Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)

Remarks prepared for delivery at the joint meeting of the security committees of the Aerospace Industries Association and the National Security Industries Association, Tucson, Arizona, May 25, 1993.

In 1988 the United States entered a new era of international arms control with consequences for the way we protect the security of Defense Department information, facilities, and industrial contractors. The ratification and implementation in 1988 of the Intermediate-Range Nuclear Forces (INF) Treaty between the United States and the Soviet Union marked the first of a series of agreements providing for foreign inspection of U.S. military and defense industry facilities. By 1993, the United States has negotiated eight major international agreements involving various forms of inspection of U.S. military facilities. These include: The INF Treaty, the Conventional Armed Forces in Europe (CFE) Treaty, the Threshold Test Ban Treaty (TTBT), the Strategic Arms Reduction Treaty (START), START II the Open Skies Treaty, the US-Russian Bilateral Chemical Weapons Agreements, and the multilateral Chemical Weapons Convention (CWC). While some of these agreements have not yet been ratified or otherwise gone into force, they contribute to a changed environment for the protection of sensitive information in the post-Cold War world.

The issue for Defense Department security programs, and for our counterparts in the Energy Department and the intelligence community, is how to balance important national interests in limitation of weapons of mass destruction, in adherence to international obligations, in confidentiality of national security information, and in avoidance of unnecessary costs to the taxpayer. The United States seeks to reduce the worldwide threats from nuclear, chemical, and biological weapons and their delivery systems through verifiable international arms control agreements. Our government is committed to full U.S. compliance with those agreements. Where an agreement requires changes in our national defense structure, we make those changes and revamp our defense acquisition programs and operational plans. We do this not only because it is a legal duty, but also because compliance by the world's most powerful nation can influence the policies of other countries. Even the perception of U.S. noncompliance could give others an excuse to violate their obligations and undermine U.S. efforts to mobilize the world against recalcitrant or defiant governments.

At the same time, there are national interests in preventing disclosure of valuable information beyond that necessary to comply with an agreement and in avoiding costly security measures to protect that information. Arms control inspections may bring trained foreign observers into facilities that have been totally off-limits to anyone lacking a security clearance. Agreements may involve the long-term presence of foreign inspectors at or near facilities that must continue to perform classified operations. They may raise the prospect of unexpected challenge inspection visits to sites that are not identified in an agreement, with varying lengths of time between notice and arrival. From a budgetary perspective, arms control inspection provisions may suggest a need for investment in upgraded security protective measures, and the impending possibility of an inspection visit may cause the costly interruption of planned tests or exercises.

The task of those responsible for security of defense information and facilities is to work with the arms control policy and implementation communities to develop inspection procedures that balance these interests properly. This means maintaining the national commitments to arms control and compliance while taking account of the need to minimize harmful disclosures and keep costs under control.

Negotiation of Inspection Provisions

These efforts begin long before an international arms control agreement is signed. During the negotiation phase, a great deal of work goes into framing positions of the U.S. negotiators that take all these factors into account. The result is the drafting of verification and inspection

provisions that do not provide unfettered access by arms control inspectors. If the sole U.S. interest were to control the weapons of other countries, our negotiations could insist upon the most intrusive verification regimes. But that is not the sole U.S. interest in arms control negotiations. The American people have invested in military capabilities that allow our leaders to achieve national goals in the world. Those military capabilities depend in substantial measure on maintaining the confidentiality of advanced systems and operational plans. Consequently, our desire to verify compliance with arms control agreements by other nations is tempered by the recognition that the verification regime ordinarily will apply to ourselves as well. Reciprocity is an integral part of the framework of international agreements that provides a means to bring greater stability and peace to a trouble world.

Negotiations have resulted in a variety of inspection measures, geared to the objectives of particular agreements. Beginning with the INF Treaty, the procedures have generally affirmed the right of the inspected party to escort visiting inspectors and confine them only to areas subject to treaty-mandated observation. The inspected party has been given the right to examine (or in some cases provide) inspection equipment so as to deter or prevent the surreptitious introduction of more intrusive devices such as clandestine technical surveillance systems. Inspection procedures have specified permissible monitoring techniques in order to limit the ability of inspectors to collect information not needed to determine treaty compliance.

Considerable care has gone into the identification of declared facilities where inspectors have observation or monitoring rights.

That was especially important when U.S. arms control objectives called for challenge inspections of undeclared facilities in order to verify foreign compliance with certain agreements. The Conventional Forces in Europe (CFE) Treaty provided for the right to conduct challenge inspections of undeclared facilities within specified areas in NATO and Warsaw Pact countries from the Atlantic to the Urals. As a result of input from defense security programs, the CFE challenge inspection regime took account of the interest in preventing intrusive observation of highly sensitive U.S. military capabilities. One provision restricted inspectors from entering doors narrower than a specified width. Another allowed the inspected party to identify a facility as a "sensitive point" when foreign inspectors arrived and thereby deny them access. The United States was willing to allow the Warsaw Part countries to have a similar right to limited challenge inspections, even though it risked making verification of Soviet compliance more difficult.

Another example is the START Treaty which contains a provision that would allow inspections of undeclared facilities, technically called "visits with special right of access." START allows a party to request a Special Access Visit (SAV) to a facility when the request-

ing party has an urgent concern relating to compliance by the other party. The procedure gives the party receiving the SAV request seven days to respond, and the response may offer alternative data or another location for consideration by a Joint Compliance and Inspection Commission (JCIC). The timetable allows as long as 47 days from initial notice to the conclusion of the JCIC session before the SAV inspection may take place. Even then, the JCIC may provide a forum for the two governments to agree that alternative data suffice to resolve the urgent concern cited by the requesting party. In short, while the START SAV inspection provision has a very broad potential scope (theoretically including purely private as well as government and government contractor facilities), the Treaty gives sufficient time to prepare for the inspection visit or to negotiate an alternative.

The CFE and START examples indicate how treaty inspection provisions have accommodated verification interests and the protection of sensitive facilities. As arms control moves from bilateral to multilateral forums and from strategic nuclear forces to chemical, biological, and conventional arms, more systematic methods are needed to analyze the impact of potential treaty provisions on the security of facilities and technologies that will maintain our battlefield edge in future regional military conflicts.

Treaty Inspection Readiness and Security Preparations

Security preparation for arms control inspections focused initially on declared facilities, where U.S. counterintelligence and security programs could assess the risks in cooperation with facility management. For the early bilateral treaties involving Soviet on-site inspection within the United States, the FBI took a leading role in counterintelligence preparation. The Soviet inspection and monitoring teams were likely to include intelligence officers (both KGB and GRU - civilian and military intelligence), and their diplomatic immunity enabled them to augment the limited Soviet intelligence presence permitted in this country under State Department controls that had tightened in the mid-1980s. Counterintelligence elements of the military services and the Energy Department worked with the FBI and with their respective installations and contractors to prepare for inspections.

The emphasis on counterintelligence was reflected in the structure of the On-Site Inspection Agency (OSIA) which was created within the Defense Department to conduct U.S. inspections in foreign countries and to escort foreign inspectors at U.S. facilities under nuclear arms control agreements and the CFE treaty. From the outset OSIA had a Deputy Director for Counterintelligence, a position filled by a senior FBI counterintelligence detailee. OSIA has coordinated its escort plans for inspections at each U.S. facility with the relevant counterintelligence and security offices, and OSIA decisions on such matters as the location of inspectors' housing took security risks into account. OSIA also arranged for technical security experts from other agencies to examine inspection equipment to be used at U.S. sites.

One of the most valuable ways to ensure the readiness of installations for on-site inspection has been mock inspections by U.S. personnel. These were initially organized by OSIA and the military service responsible for the inspected facility or, in the case of nuclear test monitoring under the Threshold Test Ban treaty, by the Department of Energy. Mock inspections became the most visible aspect of a security preparation process that looks at all the vulnerabilities of a facility to disclosure of classified or export-controlled information to inspectors. That assessment process requires knowledge of the inspectors' legal rights under the treaty, because the most cost-effective way to protect sensitive facilities may be to ensure that U.S. escorts confine foreign inspectors strictly to places they are permitted to examine. A well-prepared escort team provides vital assurance against unauthorized observation. Installation commanders, facility managers, and their security staffs also need to understand how far the inspectors will have a right to go. Based on this knowledge and the risk assessment, including mock inspection results, they have the primary task of deciding whether to relocate or shroud sensitive items or curtail sensitive activities while inspectors are present.

In 1992 the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence designated the Director, On-Site Inspection Agency, as the executive agent for a Defense Treaty Inspection Readiness Program (DTIRP) to provide support to government and contractor facilities in making security preparations for arms control inspections. Within OSIA the DTIRP is managed by the Chief, Security Office, and is integrated into OSIA planning and operations. The DTIRP receives program policy direction from the office of the Deputy Assistant Secretary of Defense (C3I) for Counterintelligence and Security Countermeasures and is integrated into the Defense-wide treaty implementation structure established in the office of the Under Secretary of Defense for Acquisition.

The DTIRP is primarily a vulnerability assessment program that brings together counterintelligence and security specialists crossing all security disciplines. The purpose is to work with facilities to identify their critical information, assess the risks to that information posed by an inspection, and develop recommended security countermeasures. The program was created to provide

timely, informed recommendations to policy decision makers, program managers, and facility managers in both government and defense industry. It is designed to foster awareness and ensure understanding that will enable all those involved to prepare effectively for treaty inspections. The DTIRP draws on personnel and support from the industrial security division of the Defense Investigative Service and from the Defense Intelligence Agency, the Military Departments, the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, and the Community Counterintelligence and Security Countermeasures Office. The principal DTIRP product is a tailored report (classified appropriately) focusing on treaty-specific vulnerabilities at inspectable sites. Also produced are special studies, database reports, and customized products.

The DTIRP can be most effective when program and facility managers have a clear concept of the critical information that requires protection. In this respect, the DTIRP and other security preparations depend heavily upon the separate procedures for security classification, for identification of export-controlled information, and for designation of Special Access Programs (SAPs). It is up to the program manager or policy decision maker to decide whether the information likely to be disclosed to foreign inspectors, as determined by a DTIRP assessment or a mock inspection, is truly critical to the national interest.

Disclosures can vary across the spectrum of risks. For instance, if the fact of the existence of a Special Access Program facility at a particular location is properly classified, indications of the presence of such a facility should be protected for the same compelling reasons that justified high-level approval of the SAP compartment under stringent statutory procedures requiring notice to key congressional committees. Other disclosure risks are not so black and white. Does visual or photographic observation of an item or process disclose classified or export-controlled information? If so, is the information so vital that it is worth the cost to relocate the item or discontinue the process — or worth the diplomatic trouble to deny access to an inspector who wants a look beneath a shroud?

In the changing world of the 1990s, not everything we tried to keep secret from the Soviet military in the Cold War may still need protection. A recent initiative to refine the Defense Department's information protection policies in light of these changes is the Acquisition Systems Protection Program. It seeks to bring together acquisition program offices, security specialists, and intelligence and counterintelligence analysts to develop a protection plan that identifies essential program information, technology, or sub-systems requiring protection at each stage of the life of the program. Protection plans should provide more cost-effective security for advanced weapons systems by improving classification and foreign disclosure decisions. Protection planning and treaty inspection readiness are partners in developing better risk management methods for the post-Cold War environment.

The Open Skies Treaty

The DTIRP showed its value as the focal point for assessment of the risks from the Open Skies Treaty and for development of a security countermeasures initiative adopted by the Defense Department's Open Skies Treaty implementation manager. Open Skies is a multinational confidence and security building measure designed to provide mutual assurances among its 25 signatory states who are the members of NATO and the members of the former Warsaw Pact including four states coming out of the former Soviet Union — Russia, Ukraine, Belarus, and Georgia. The treaty allows for the unimpeded overflight of all territory of the signatory states, including the United States. Open Skies flights may collect imagery from frame, panoramic, infrared, and synthetic aperture radar sensors. For some, this is a collection capability they never had. For others, it increases their capability over certain commercially available sources. For still others, it represents an additional capability to complement existing collection systems.

The parties signed the Open Skies Treaty in March, 1992, and an Open Skies Consultative Commission com-

pleted work on sensor details in June, 1992, opening the way for countries to ratify the treaty. As with other agreements, the Open Skies Treaty contains provisions that assist security preparations. An observed party must receive notice of an observation flight at least 72 hours before its arrival at the point of entry, and the period from estimated arrival until completion of the flight cannot exceed 96 hours, unless otherwise agreed. The observed party has a right to inspect the sensors and may require a demonstration flight. The host country also has a right to have its own aircraft used for the flight.

The DTIRP has focused on developing a capability to provide early warning by datalink, fax, and autodialer telephone to sensitive government and contractor facilities along the proposed path of an Open Skies flight. Absent such notice, program and facility managers informed of the arrival of an Open Skies flight in the United States would have to consider costly suspension of tests and exercises throughout the country. With the help of a Defense Nuclear Agency compliance RDT&E initiative, the DTIRP solved the problem by taking an established technology, the Northrop Mission Planner, and developing requirements for an automated capability to analyze a planned overflight route and predict sensor coverage. The new system is called the Passive Overflight Module. When linked with a site database and other DTIRP Treaty database information, the module can support risk assessment and early warning/notice requirements. Government and contractor facilities that should have notice will be included in the system, and there is capacity to add purely private facilities if authorized.

The DTIRP Passive Overflight Module also has the capability to conduct postflight analysis. If an Open Skies flight goes off its planned course, the sensors should be turned off. But weather and other factors may result in some deviation from planned sensor coverage. Facilities observed without prior notice, or observed more closely than expected, can be informed afterwards in order to assess the possibility of compromise. Another benefit of post-flight analysis is to determine whether another country may be using Open Skies flights to spot locations for challenge inspections under START of the Chemical Weapons Convention. Indeed, the preamble of the Open Skies Treaty specifically mentions its potential for use in monitoring compliance with other treaties. This linkage between treaty inspection provisions has raised concern that a foreign government could use the synergy among treaties to develop collection targeting plans against sensitive U.S. facilities. The DTIRP system provides the analytical tools to assess Open Skies flights and other inspections for indications that another country is exploiting treaty synergy.

Designed to help end the Cold War, Open Skies will be implemented in a very different risk environment. The Soviet Union would undoubtedly have tried to exploit the linkage among treaties to compromise U.S. military secrets. The risks today are different and have less serious consequences without the specter of great power conflict. There is concern about technology theft and industrial espionage by a variety of countries, with consequences harmful to counterproliferation efforts and U.S. economic interests. The data gathered from any Open Skies flights by former Warsaw Pact countries over U.S. territory will be available to all 25 signatories. It will be easier for a foreign government to obtain any available Open Skies data from coverage of U.S. territory than to run the diplomatic risks of mounting a collection effort using similar sensors on a private aircraft in civil air space.

The prospects for Open Skies implementation are uncertain. The financial burdens may reduce the likelihood of very many flights by former Warsaw Pact countries, especially with the East European desire for U.S. assistance. Nevertheless, the Defense Department has the responsibility to make preparations for Open Skies that will minimize the risks to sensitive facilities.

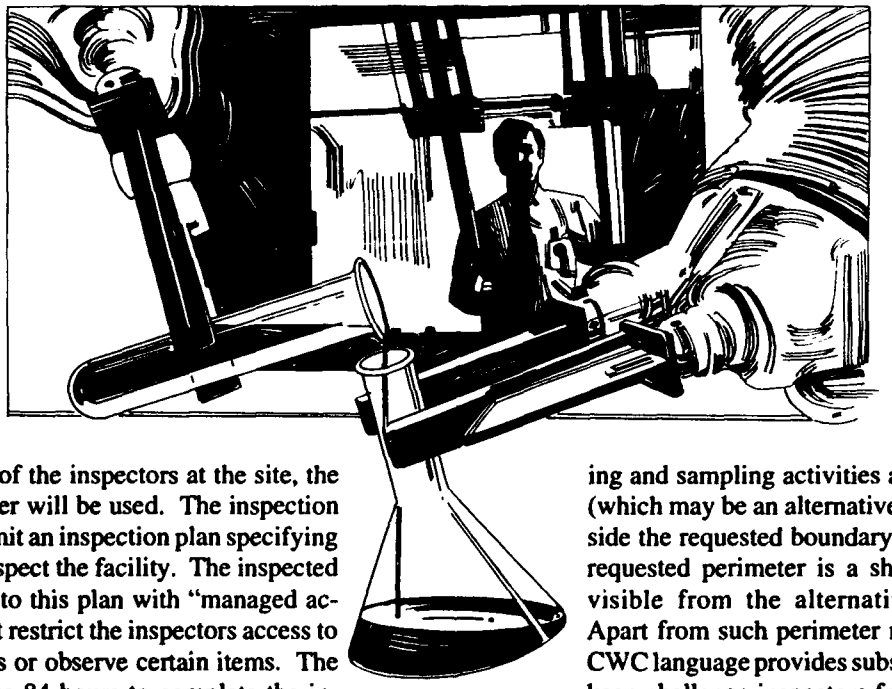
The Chemical Weapons Convention

In January, 1993, over 130 countries including the United States signed the Chemical Weapons Convention (CWC) which obliges the parties never to develop, produce, stockpile, or use chemical weapons. The parties are required to destroy all chemical weapons within ten years after the CWC enters into force and to destroy or convert for peaceful commercial use all former CW production facilities. The CWC verification regime includes inspections of declared facilities and short-notice challenge inspections at declared and undeclared sites to resolve suspicions of non-compliance. (A separate bilateral agreement between the United States and the Russian Federation has yet to be formally approved but was reaffirmed by Presidents Bush and Yeltsin in 1992. Its inspection provisions are similar, but narrower in scope.)

The CWC short-notice challenge inspection provisions have occasioned great interest, but risk assessment must take into account the significant differences between the CWC and previous arms control agreements. The inspections will not be conducted by a foreign government with the ability to direct and staff inspections for intelligence-gathering as well as verification purposes. Instead, the inspections will be conducted by an international Organization for the Prohibition of Chemical Weapons, and the treaty calls for security procedures to protect confidential information obtained during inspec-

tions. While foreign intelligence services may penetrate the organization, it will be more difficult for them to exploit inspection access systematically.

As with previous treaties, the CWC challenge inspection provisions take account of the need to protect the security for sensitive facilities and information. The inspected state must be notified of the location of the inspection site not less than 12 hours before the planned arrival of the inspection team at the point of entry into the country. If the requested perimeter of the site is not acceptable to the inspected state, it may propose an "alternative perimeter" meeting certain criteria within 24 hours after the inspection team arrives at the point of entry. If perimeter negotiations reach no agreement within 72 hours after arrival of the inspectors at the site, the alternative perimeter will be used. The inspection team will then submit an inspection plan specifying how it wishes to inspect the facility. The inspected state may respond to this plan with "managed access" measures that restrict the inspectors access to enter certain spaces or observe certain items. The inspectors will have 84 hours to complete the inspection unless extended by mutual agreement of both sides. The time between notification to the start of the inspection can take up to five days.



At the perimeter of the CWC challenge site, inspectors may use specified monitoring instruments and take wipes, air, soil or effluent samples. All directional monitoring must be oriented inward. Within the perimeter the access of the inspection team will be negotiated with the inspected state "on a managed access basis." The inspected state is "under the obligation to allow the greatest degree of access, taking into account any constitutional obligations it may have with regard to proprietary rights or searches and seizures." In addition, the inspected state "has the right under managed access to take such measures as are necessary to protect national security." If the inspected states "provide less than full access to places, activities, or information, it shall be under the obligation to make every reasonable effort to provide alternative means to clarify the possible non-compliance concern that generated the challenge inspection." The CWC lists examples of measures that may be taken "to protect sensitive installations and prevent disclosure of confidential information and data not related to chemical weapons." It also lists examples of actions that may be taken to respond to non-compliance concerns, e.g., "the partial removal of a shroud, at the discretion of the Inspected State Party [or] a visual inspection of the interior of an enclosed space from its entrance."

The CWC challenge inspection provisions give the United States wide discretion to limit inspections by using alternative perimeters, managed access, and the right to substitute reasonable alternative means. The only unqualified authority of an inspection team is to conduct monitoring and sampling activities at the perimeter (which may be an alternative perimeter outside the requested boundary, so long as the requested perimeter is a short distance or visible from the alternative perimeter). Apart from such perimeter monitoring, the CWC language provides substantial rights to keep challenge inspectors from gaining access to classified or export-controlled information.

Nevertheless, it may not be in the interests of the United States to exercise these treaty rights to the fullest extent, especially if a U.S. effort to limit CWC challenge inspections would encourage other countries to resist challenge inspections that are necessary to achieve U.S. counter-proliferation goals. Senior U.S. policy decision makers may take such factors into account in determining how to respond to a particular CWC challenge inspection. For that decision to be made with sufficient knowledge of the consequences, however, defense program and facility managers should have a clear idea of the critical information they would most need to protect from a CWC challenge inspection.

To prepare for CWC inspections, the Military Departments and the DTIRP are providing training, risk assessments, mock inspections, and compliance planning guides. The DTIRP is assisting non-DoD agencies and government contractors. Coordinated preparation for

CWC challenge inspections is especially important to ensure that policy decision makers will have a common terminology and risk assessment framework for determining how to exercise U.S. treaty rights. Careful planning is also needed to ensure prompt and efficient communication among affected components and policy decision makers who must provide guidance to meet the short time deadlines.

The extent to which U.S. facilities will be subject to CWC challenge inspections is difficult to predict. The multinational executive Council of the Organization for the Prohibition of Chemical Weapons will have the authority to disapprove a challenge inspection request as "frivolous, abusive or clearly beyond the scope of this convention." The decision requires a three-quarter majority vote of the Council and must be made not later than 12 hours after receipt of the inspection request. Thus, the United States has an opportunity to prevent challenge inspections by invoking this procedure. A larger question is whether any state parties will have the incentive and the resources to gather information for the purpose of alleging U.S. noncompliance. One potential incentive would be retaliation against a challenge inspection conducted at U.S. request. In that situation, however, the United States would have strong grounds to justify exercising its treaty rights to the fullest extent. It is also worth noting that if after a challenge inspection the executive council finds the request for an inspection to be outside the scope of the CWC or that the right to request an inspection was abused, then the requesting state party may be required to pay for the inspection. This, too, may deter frivolous inspections.

The uncertain likelihood of CWC challenge inspections at U.S. facilities does not mean preparation is unnecessary. To the contrary, risk assessments based on an understanding of treaty provisions and coordinated policy guidance should prevent facilities from taking costly security precautions. Verification experts can identify those types of features of a facility most likely to be of interest to CWC inspectors. A basic knowledge of treaty concepts and procedures should be incorporated into the training of security personnel throughout the government and the contractor community. Challenge inspection contingency plans should be an integral part of protection planning at sensitive facilities regardless of CWC challenge inspections. The open international environment increases the likelihood of a variety of other types of foreign visits to military and contractor installations. Better security planning is needed to make informed decisions on access control in a wider range of situations.

In the final analysis, the lesson of treaty inspections is that program and facility managers should think carefully about their protection priorities. We can no longer classify by rote, deny access wholesale, or afford the cost of protection against every marginal vulnerability. The Deputy Secretary of Defense, Dr. William Perry, has identified security restrictions as one of the barriers to reforms of the defense acquisition system that are necessary to reduce overhead costs and increase emphasis on technologies with dual military and commercial uses. The Administration has initiated an interagency review of the classification Executive order and has formed an advisory commission to review the security practices and procedures of the intelligence community and the Defense Department. These efforts should improve the methods for identifying critical information and setting protection priorities. Improved security management can, in turn, make it easier for the United States to know when to take greater risks in order to achieve arms control and counterproliferation objectives through verifiable international agreements designed to bring about a safer world.

Industrial Security Management Course

White Sands Missile Range New Mexico

To enroll, mail this page to: Commander, U.S. Army
Attn: STEWS-SD-S (MARQUE
White Sands Missile Range
New Mexico 88002-504

Or call: Art Marquez at (505) 678-4502

Title of Course: *Industrial Security Management Course*

Location: White Sands Missile Range, NM **Course Dates:** Aug 9 - 12, 1993

Your Name: Mr. Mrs. Ms. _____
(circle one) (Last), (First)

Job Title: _____ **Military or GS Grade:** _____

Social Security Number: ___-___-___ **Date of Birth:** _____

Business Address:
_____ **Supervisor:** _____
_____ **Supervisor's Phone:** (___) ___-____
_____ **Your Phone:** (___) ___-____

August 9 - 12, 1993

Call Today!

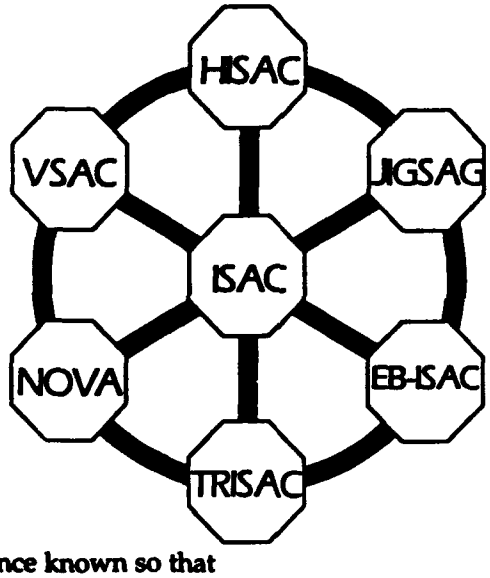
Applications will be accepted by phone through August 6.

Industrial Security Awareness Council (ISAC) Network

by Gussie Scardina

The January 1991 Security Awareness Bulletin described contractor efforts at forming security awareness groups throughout the country and promised to publish regular updates on regional group activities. The number of groups has grown significantly and their memberships have expanded to include various government agencies. The purpose of this article is to update the listing of these groups, offer the Security Awareness Bulletin as a vehicle for announcing the activities planned by these groups, and establish an ISAC network.

In order to be able to do any of the above, input is required. Sometime before Thanksgiving, all of the "known" ISACs, i.e., those listed below, were contacted and asked to provide some information about themselves . . . where they are located, why they formed, what they have accomplished or plan to accomplish, who's involved, etc. Many provided some GREAT information. Others provided NO information. (You know who you are!) This is your group's chance to make its existence known so that it may benefit from the experience of others. Give us "the scoop" so we can pass it on! And so begins the ISAC network . . .



These descriptions are written (nearly verbatim) from the information provided by members of the following:

Greater Los Angeles ISAC

Sharing Security Resources is the motto adopted by our group. In 1988 we named ourselves, ISAC, short for Industrial Security Awareness Council. No further distinction was necessary because we were the only one in existence. The council was established because a need existed to provide better security education with fewer dollars and other resources. We all had the same mission. Why not pool those limited resources and make them work harder and go further?

That was over four years ago and a lot has happened in those four years. Two of our founders have gone on to bigger and better things — Greg Gwash is now at DIS Headquarters and Rusty Capps is at FBI Headquarters where they encourage their respective agency personnel to participate in similar groups. Since now there are over 20 ISACs around the country, it was necessary to add "Greater Los Angeles" to our name.

In January 1991, the Security Awareness Bulletin included an article featuring this ISAC as well as other similar groups that were forming around the country. Many of our projects and products were discussed. Since then, the council has continued to provide programs and materials to the local companies. Highlights of some recent activities are described below:

The Security Education and Awareness Committee continues to provide printed materials and has recently printed their fifth poster.

The seminar committee had a very busy year in 1992. They put on a PSQ seminar, two Security Briefers Courses, and our fourth annual FSO seminar. This is one of our most productive groups. So far this year, they have conducted a half day Security Education Workshop and two Security Briefers Courses. The response to all of these events has been excellent. Take note of their upcoming events on the attached 1993 agenda calendar.

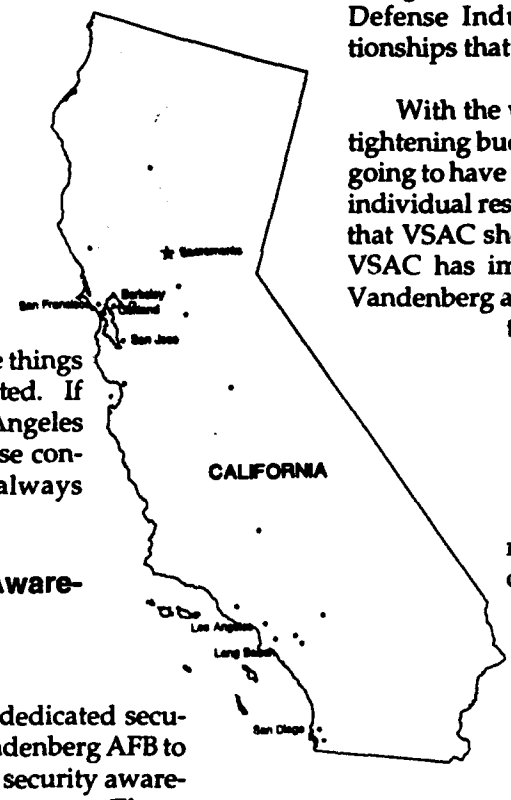
A recent addition to our archives is a new video produced by Hughes and titled "Friend and/or Foe."

Application for incorporation with the state of California is in process to formalize and protect our

"non-profit organization" status with the state franchise tax board and the Internal Revenue Service.

And we aren't above stealing, or rather borrowing, good ideas from other groups. After all, that's what the ISAC is all about. Therefore, we have decided to follow the lead of several other ISACs and have published a quarterly newsletter. The first edition hit the streets in March 1993 and has been sent to our sister organizations.

Each of these committees includes a cadre of very hardworking, dedicated people all striving for the same goal—an excellent security awareness program that benefits everyone, large companies and small. This is by no means all of the things going on, but space is limited. If you are in the greater Los Angeles are and are interested, please contact us. Volunteers are always needed and welcome.



Vandenberg Security Awareness Council (VSAC)

In March 1991, several dedicated security professionals met at Vandenberg AFB to discuss how to improve the security awareness in the Vandenberg area. These individuals' goals were to help each other by sharing resources and time in an effort to make security education more efficient. The result was the VSAC.

The VSAC is an informal, non-profit association of defense contractors, the Department of the Air Force, the FBI and the DIS. These organizations have joined together to promote security awareness in the Defense Industry by focusing the collective energy and resources of industry and government in the Vandenberg area. It is agreed that none of us can do it alone.

Objectives:

1. Act as a clearinghouse to more effectively manage resources and reduce duplication.

2. Create awareness programs that relate to the Vandenberg area.

3. Enhance the realization of company managers and employees that sound security practices are essential to contracts, profits, and jobs.

We are located in a high target profile area; a direct result of Vandenberg Air Force Base and the high technologies associated with it and in the surrounding vicinity. We are also blessed with close working relationships between Government and the Defense Industry. It was out of those relationships that VSAC was formed.

With the world situation as it is and an ever-tightening budgetary belt, it was evident we were going to have to provide more training with fewer individual resources. It was a logical progression that VSAC should become a reality. As a result, VSAC has improved security education in the Vandenberg area and has reduced costly duplication of effort.

Accomplishments:

1. Providing material and information for the Quarterly Facility Security Officers Meeting.

2. Hosting a workshop on new security forms, DD Forms 398, DD Forms 398-2 and DD Forms 1879 conducted by Mrs. Linda Kimbler of DIS.

3. Sponsoring an ISM Requirements and Security Education Seminar conducted by Mr. John Frields, Deputy Director Industrial Security, OSD and Mr. Jim Linn, Corporate Security Manager, SAIC.

4. Presenting a half day Security Awareness Seminar covering such topics as the Threat and OPSEC.

5. Participating in and teaching DoDSI's Train-the-Trainer/Security Briefers Course.

6. Designing, reproducing, and distributing security awareness posters.

7. Maintaining a library of security awareness videos and educational materials.

8. Publishing and printing awareness pamphlets.

9. Creating and distributing a quarterly newsletter.

San Francisco Bay Area (SFBA) ISAC

The SFBA ISAC began in 1991. A needs assessment survey was distributed to Bay Area companies asking for their input regarding security awareness needs. The first committee meeting was held in the summer of 1991. Meetings are now held every other month.

The purpose of the ISAC is to promote security awareness in the defense industry by focusing the collective energy and resources of San Francisco Bay Area industry and government entities. This mission will be accomplished by achieving the following objectives:

1. Act as a clearinghouse to more effectively manage resources and reduce duplication.

2. Create awareness programs which can reach smaller defense firms.

3. Promote an appreciation that sound security practices support sound business practices.

The SFBA ISAC has developed a 1992 Reference Manual that includes a listing of those companies which have or are willing to share their security education materials and publish a quarterly bulletin. Its members have sponsored seminars on security awareness programs and materials including a presentation by the FBI concerning the present threats to national security. A calendar of security related events is also in the works.

North Bay ISAC

Industrial security professionals in the North Bay counties of California started their own ISAC in the region which has previously had little access to the many professional organizations that exist in more populated areas of the Northwestern region of DIS. Formed in 1991, the North Bay ISAC has chosen to devote its first efforts to security education. The group has created a Desk Top Guide and complied a list of security education materials available through it members. It has developed an Initial Briefing Outline and is currently working on a Foreign Travel Briefing. They have approximately 20 members, meet every other month and are hoping to increase the size and participation of the group. Defense contractor security personnel in Marin, Sonoma, Solano, Napa, Lake, and Mendocino counties are encouraged to join .

East Bay ISAC (EB-ISAC)

The purpose of the EB-ISAC is to promote security awareness in the defense industry by focusing the collective energy and resources of industry, education and government in the East Bay Area. This mission will be accomplished by achieving the following objectives:

1. To act as a clearinghouse for the free exchange of information.

2. To act as a focal point to stimulate industrial security awareness.

3. To promote sound security practices.

Minutes from previous meetings reveal that the initial meeting of this ISAC, held on June 23, 1992, determined the following:

1. The organization would not be formal with elected officers, etc., but chaired each time by the host location for the meeting.

2. Meetings would be held quarterly.

3. Three committees were formed . . . the Logo Committee, the Mission and Objectives Committee, and the Research and Ideas Committee.

Central Valley Chapter ISAC

The purpose of the ISAC is to promote security awareness in the defense industry by focusing the collective energy and resources of the Central Valley area industry and government entities. This mission will be accomplished by achieving the following objectives:

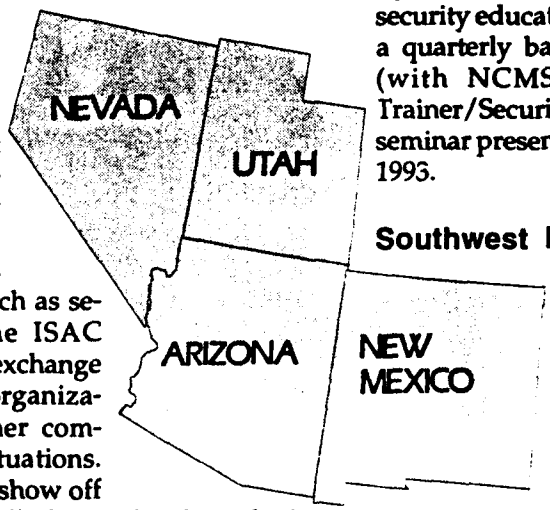
1. Act as a clearinghouse to more effectively manage resources and reduce duplication.

2. Create awareness programs which can reach and assist smaller defense firms.

3. Promote an appreciation that sound security practices support sound business practices.

Our ISAC meets informally once per quarter with the host chairing the meeting and arranging the agenda. Our meetings are round table discussion with members exchanging experiences, both positive and negative, that have impacted on their companies' security postures. We exchange posters, procedures, inspection checklists, and brochures. Many of our chapter's members are from very small facilities and have limited resources for security. This exchange of information and material is their primary source of security subject matter. We are currently considering conducting a one or two day training seminar within the next 12-18 months for the smaller DoD contractors within our chapter area. We intend to have DIS, FBI, and DoD contractor personnel provide instruction in security education and training, the foreign threat, classification management, physical security and safeguarding, automated information system (AIS) security procedures, and any other subject deemed necessary. Our intent is to keep our ISAC very informal and rely on the spontaneity of each member to provide a forum where we feel comfortable exchanging ideas or seeking assistance. To keep our members informed we have begun publishing minutes of our meetings.

Silver State ISAC



Our ISAC had its first meeting in July 1992. We now have approximately 15 members who meet on a quarterly basis to discuss various security topics, such as security inspections. The ISAC provides us a chance to exchange information about our organizations and share how other companies handle various situations. We get the opportunity to show off what our companies are all about. We have had training presented by the FBI and have established a videotape library from which our members may borrow security education tapes. Our local IS Rep is always available to answer any questions afterwards and to share publications or current events. The meetings are always very informative and helpful.

Phoenix ISAC

This group was established as a contractor-driven organization. The primary goal of this ISAC is to serve as an unofficial contractor network to answer questions or help solve problems related to the Defense Industrial Security Program. It meets on a quarterly basis. Prior to completion of a meeting, a consensus is reached on what topics are to be discussed at the next meeting. After the topics have been chosen, resources are volunteered to support the discussion of those topics; e.g., if AIS is chosen, the regional DIS AIS specialist will be invited to attend the next meeting. The group is co-chaired by the Senior I.S. Rep from the local field office and an industry representative. This ISAC has networking in mind for solving problems and answering questions in addition to conducting round table discussion/workshops at the quarterly meetings.

Salt Lake City ISAC

The Salt Lake City ISAC was formed in March 1991 and functions as a subcommittee of the Intermountain Chapter of the NCMS. Membership in the ISAC is comprised of all defense contractors in the Utah area.

The ISAC has an extensive security education library which is available to all contractors and mails security education materials to all contractors on a quarterly basis. In October 1992, the ISAC (with NCMS) sponsored the Train-the-Trainer/Security Briefers Course and a two-day seminar presented by DoDSI instructors in April 1993.

Southwest Industrial Security Council (SISC)

The SISC was born in July 1988 to fill a void. There were simply no industrial Security organizations in the area dedicated to enhancing our security expertise. With a list of names and addresses, we were on the road to developing our own professional organization.

If you talked to ten different members of our group you would probably get ten different answers as to what is the most important thing they have gained from being a part of this organization. One answer would have to be people! Prior to the formation of our organization some may have not known who the FSO for Bendix was; now we think "I'll call Bill; he might give me some insight to this problem I am trying to solve." Through the SISC, we know

each other and are able to gain knowledge from each others' experiences.

We normally meet the third Thursday of each month at 10:00 a.m. Sometimes we vary the time so we can have a luncheon meeting. Occasionally we may change the date to accommodate the schedule of a guest speaker. Each month a member will volunteer to host the next meeting, so our meetings have rotated to various sites on the White Sands Missile Range Main Post, the NASA Site, HELSTF, HAFB and Alamogordo.

We take turns in obtaining guest speakers or in presenting the topic for the meetings. The White Sands Security Directorate (WSSD), the Dallas office of DIS, the FBI and the Las Cruces Police Department are some of the organizations that have been responsive to our requests for presentations.

We have chosen to remain a very informal organization. Donations are taken at each meeting to cover the cost of mailing the monthly newsletter. The job of preparing the monthly newsletter has also been shared among the members of the organization. We also help in the preparation for the annual Industrial Security Seminar sponsored by the WSSD at the Holiday Inn de Las Cruces.

Advantages of being a member of our informal organization include:

Training and education

Sharing of training material

First-hand information for possible career advancement

Knowledge sharing

Support

Improved customer service

Camaraderie with other security professionals

If you believe the SISC would benefit you and your organization please contact us. We know we will benefit from your expertise. We will be looking forward to hearing from you.

ISAC — New Mexico

The ISAC -- New Mexico was established to increase the lines of communication among government and industry security professionals. Under its charter, the ISAC:

Promotes to industry managers and employees that security education, training and awareness is essential to profits, contracts, and corporate performance.

Creates security education, training and awareness programs and resources which can be made readily available for use by contracting firms with limited resources and education programs.

Acts as an information center that will effectively manage existing and newly created programs and resources to provide guidance and tools for use by organizations seeking to enhance their security education, training and awareness programs.

The ISAC supports and promotes the development and sharing of security education, training and awareness materials and programs of general benefit to both industry and government participants. The ISAC will continually develop and update security training forums and briefings to include the Foreign Threat; Safeguarding, Marking and Destruction; COMSEC; OPSEC; and a variety of other vital security issues.

The ISAC interacts with major industry and government security education, training and awareness organizations throughout the country. The ISAC — New Mexico is a standing committee of the Enchantment Chapter of the National Classification Management Society (NCMS). The ISAC draws upon the extensive resources of the NCMS to help accomplish its mission. NCMS membership, while encouraged, is not required to be an ISAC participant.

The ISAC has a steering committee which meets at least quarterly to review and plan ISAC initiatives. The steering committee also determines the parameters of "association" with existing professional societies and organizations with interests similar to the ISAC. Volunteer working group chairs are automatically members of the steering committee. All ISAC members are encouraged to serve on one or more volunteer working groups. The more members involved, the less time needed by any one individual. Our goal is a totally cooperative and participatory council.

The ISAC has sponsored "Security Round-Ups", FBI DECA briefings, STU III workshops, and supported NCMS seminars conducted in the local area.

Rocky Mountain Region (RMR) ISAC

The RMR ISAC was established in 1990 by a small group of Colorado contractors led by Education Specialists from Martin Marietta Technologies, Inc. Astronautics Group. Since that time, leadership initiatives have broadened with the involvement companies such as Ball Aerospace, Science Applications International Corporation, U.S. West and others.

The RMR ISAC is comprised of a general council and various subordinate working committees. The general council consists of eight contractors and one representative from the FBI and the DIS. The council usually meets about every two months to provide organizational oversight as it decides policy and determines direction for the ISAC. The participation of the area's FBI DECA Representative on the council provides members of the group with current espionage and counterintelligence information as well as presenting outstanding and motivating DECA briefings on-site to contractor employees.

In striving to reach its goal of enhancing national security awareness, the RMR ISAC has identified three organizational objectives:

To establish joint industry-government cooperative security efforts to make better use of security resources industry-wide

To identify and support the security needs of defense contracting firms

To enhance company management and employee understanding that sound security practices are essential to national security, jobs, contracts and profits.

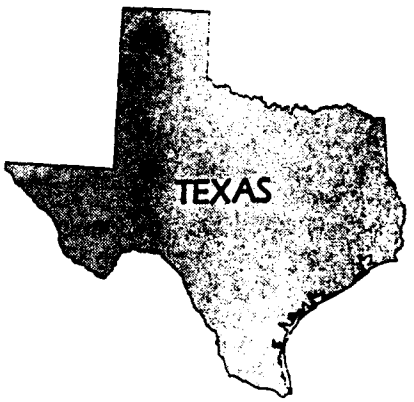
Accomplishments for 1992 included hosting a Susceptible Traveler Program and a Train-the-Trainer/Security Briefers Course, expanding the ISAC library and publishing an ISAC newsletter.

1993 initiatives include more aggressive advertising with greater emphasis on membership involvement. Specific goals for the future include: determining the training needs of industry; working to increase contractor awareness to ISAC capabilities; increasing ISAC — FSO involvement in ISAC projects; providing contractors with seasoned security points of contact in industry; creating an ISAC membership base; and updating an ISAC training resources index.

North Texas Joint Security Awareness Council (JSAC)

This JSAC was formed in January 1992. The council is chartered to combine the human and material resources of the government and defense contractor communities to better serve the mission of security education and awareness.

Council membership is open to any cleared contractor facility or government entity which is associated with the security community. A twelve member steering committee oversees the routine business of the council and votes on motions placed before the council.

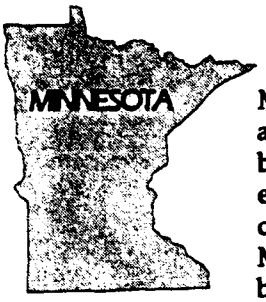


In April 1992, the council sponsored its kick off meeting at Naval Air Station, Dallas, TX. In addition to a JSAC introduction by Jim Bass, Dan James, FBI Special Agent and ISAC member, presented a DECA briefing; Richard Modesette, Department of Commerce Export Enforcement spoke on export controls and Joe De Gregorio, Director of Industrial Security for the DIS Southwestern Region provided valuable updates on issues in the Industrial Security Program. Approximately 160 government and industry representatives attended the symposium and initial feedback was favorable.

In September, the JSAC with DIS and NCMS jointly sponsored an international affairs symposium. Topics included export administration, international aspects of the National Industrial Security Program and defense trade regulations. Planned future events include coordinated efforts with the Florida East Coast ISAC to provide special briefings on magnetic media available to industry and a general topics workshop/symposiums planned for smaller contractors who may not have

full time security professionals in the facility security officer (FSO) position. Depending on the success of the workshops locally, a training team may elect to repeat the training in the Tulsa or Oklahoma City areas.

Minnesota ISAC (MISAC)



The purpose of the MISAC is to promote security awareness within industry by focusing the collective energy and resources of industry and government in Minnesota. This mission will be accomplished as we:

Act as a clearinghouse to effectively manage resources and reduce duplication.

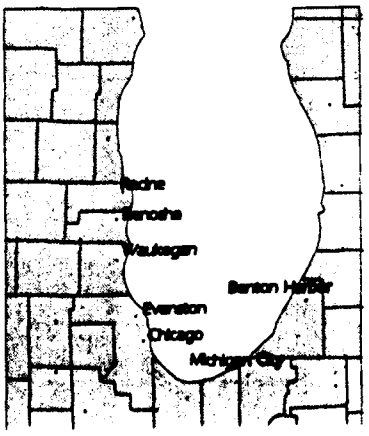
Emphasize educational awareness programs that can be used by all organizations regardless of size.

Enhance the realization by management and employees that sound security practices are essential to contracts, profits, jobs and national security.

Our ISAC is comprised of 42 organizations with representation from the local and regional DIS offices as well as 1 state and 3 federal agencies. We meet every other month, publish a newsletter and have sponsored training on the FAA requirements for couriers of classified material; susceptible traveler awareness; patent, secrecy, and proprietary information protection; and hostage crisis situations and intervention. Our major goal is to compile an extensive resource library from the training aids utilized by all of our members and other ISACs.

ISAC — Chicago

The ISAC Chicago (ISAC/C) is a cooperative whose objectives are to promote and assist security education and training efforts within its member organizations. Membership is open to any person, firm or corporation in the Greater Chicago, Illinois area whose business interests require (or would benefit by) a security education and/or awareness program. If you believe you can benefit from and contribute to the ISAC, please join us.



Huntsville (HISAC)

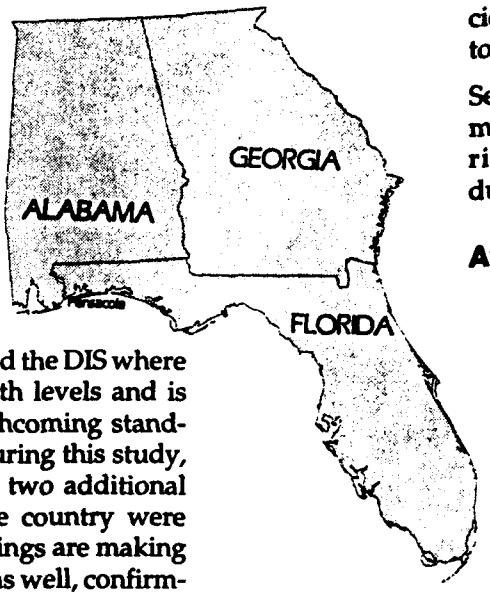
In response to the success of the Los Angeles area ISAC and other councils formed around the country, a Huntsville area ISAC was initiated in July of 1990 for the purpose of enhancing security awareness throughout the greater Huntsville area. Our goals are to enhance security awareness in the Huntsville contractor/government community, serve as an open forum which will identify and work to resolve security vulnerabilities and inefficiencies occurring in contractor/government relationships and to serve as a clearinghouse to more effectively manage finite security resources and reduce duplication of effort (i.e., avoid reinventing the wheel).

The HISAC is an informal association of defense contractors and government activities including the DIS, FBI, US Army Missile Command, Missile, Space and Intelligence Center, NASA, US Army Strategic Defense Command. The council is not a general membership organization, but meetings are open to visitors and committees are formed from non-member volunteers.

The greatest benefit is the open forum that exists at the meetings. Here, contractor FSOs can express their concerns and problems directly to government security and DIS reps who are in a position to change or influence change for the benefit of all companies. The dialog and exchange of ideas is positive and productive; many solutions are worked out and implemented without any fanfare or credit.

During the short life of the HISAC much has been accomplished. In concert with DIS, a survey of the facilities categorized as D and E was made and training offered in a two-day seminar. The seminar was taught by members of the HISAC committee and DIS I.S. Reps. Approximately 30 attendees availed themselves of this free training. Plans are to conduct a similar training seminar in the future for new FSOs primarily from small companies in Northern Alabama. Another issue was addressed last summer by the HISAC Subcommittee on Intelligence. This subcommittee met weekly during June through August and made an in-depth study of the controls prescribed by DCID 1/7 and other User Agency

interpretations imposed on contractors when required to utilize "intelligence" information during contract performance. As we all know, the varying, and sometimes conflicting, interpretations by all parties created a state of confusion when handling intelligence information. The subcommittee submitted its findings to the HISAC, and subsequently to both Headquarters Department of the Army and the DIS where the report has been accepted at both levels and is expected to be instrumental in forthcoming standardized instructions to industry. During this study, it was also discovered that at least two additional organizations in other parts of the country were studying the same issue. Their findings are making their way through official channels as well, confirming that this issue is not limited to just this area, but is a national issue for contractors.



South Florida ISAC

An initial meeting was held at UTC Pratt Whitney on May 20, 1993. Representatives from the Florida East Coast ISAC, the FBI, the CIA, the Defense Logistics Agency (DLA) and several area contractors were in attendance. An acting chair was designated until an election is held.

Florida East Coast ISAC

Formed in April 1991, the Florida East Coast ISAC is an informal association of security professionals dedicated to promoting security awareness within industry and government on the Florida East Coast, Puerto Rico and the Caribbean Basin areas.

Our members, elite in the areas of industrial, information, personnel and physical security, represent Boeing, Rockwell International, Harris, McDonnell Douglas, Computer Sciences Raytheon, Grumman, Lockheed, NASA, Air Force and the DIS. Our membership provides us immediate access to a wealth of security knowledge.

Our goals include:

Enhancing security awareness in the local contractor/government community.

Serving as a forum which will identify and work to resolve security vulnerabilities and inefficiencies occurring during contractor/government relationships.

Serving as a clearinghouse to more effectively manage security resources and reduce duplication of effort.

Atlanta Area — TRISAC

The Atlanta area ISAC, established in February 1991, was comprised of representatives from North Carolina, Tennessee, and Georgia, thus, the acronym TRISAC. The TRISAC presently consists of 18 active members including representatives from the FBI, Robins and Arnold AFBs, DIS, and eleven cleared contractors.

The parent group meets once a quarter and is presently chaired by Mr. Robert F. Lang, Facility Security Officer, Georgia Institute of Technology. Due to the wide geographical area the TRISAC encompasses, two very active subgroups have been established at Arnold AFB, TN and Warner Robins AFB, GA. These subgroups permit a wider dissemination of information and have been well supported.

Products developed by the TRISAC include an Audio-Visual Training Aids Catalog, a Security Speaker Bank and the Mentor/Protégé Program.

The TRISAC has sponsored an AIS Security Procedures for Industry Workshop in the Atlanta area and is scheduled to host the Train-the-Trainer/Security Briefers Course in September. They are hoping to develop a handbook on technology transfer and would appreciate any input, products, suggestions, and expertise in this area.

Dulles Area Security Awareness (DASA)

I-66 Corridor Security Awareness Group

Tyson's Area League of Industrial Security Managers (TALISMAN)

All of these groups are similarly structured. Each has an informal steering committee of 3-5 individuals who determine the agenda and record minutes, etc. The general purpose of the groups is to promote the exchange of information by serving as a

resource group of area FSOs who discuss common security problems and other security related information.

Joint Industry-Government Security Awareness Group (JIGSAG)

The JIGSAG is a grass roots organization of industry and government security professionals focusing on hands-on training and education. We (1) find out what our colleagues want to know (2) identify sources within industry, government or both, for this needed knowledge and expertise and (3) provide a forum to present this information. The forum may be a newsletter article, a workshop, a seminar or a "fact" sheet.

We disseminate a JIGSAG Newsletter, an International Threat Subcommittee Report and a Computer Virus Clinic. The Newsletter is published three times a year; the others are published as time and "volunteerism" permit. Our newsletter provides information about the existence of other organizations with potential benefit to our colleagues and announces upcoming JIGSAG events in addition to other security related education, training and awareness events being hosted by other organizations. If you have security related information which would be beneficial to your colleagues, we will accept your articles for publication.

We provide information (without endorsement) about products and services which are available to security professionals. We support and promote organizations such as the NCMS, the American Society for Industrial Security (ASIS), and the OPSEC Professionals' Society as means of professional development and career enhancement.

We sponsor the Security Briefers Course; a three-part *AIS workshop; a STU III/Secure Fax workshop;* an OPSEC seminar; and a two-day Security Professionals' seminar. We are in the process of putting together a "Lockshop" (Physical Security) workshop. We have published the JIGSAG Compendium, a collection of topics for security briefings and review security videos as part of the Aerospace Industries Association/DoDSI security products clearinghouse project.

We are security professionals who have come together as a means of using our collective energy and resources to facilitate security education, training and awareness. We are an "open" organization always looking for people who want to participate with us.

Northern Virginia (NOVA) ISAC

The kick-off meeting of the newly formed NOVA ISAC was held on April 20, 1993. Its aim was to establish the overall goals for the ISAC, identify its objectives and determine the common areas of concern/ideas to share.

The major goals are to:

Improve the security programs in Industry.

Increase the understanding of Industry and Government perspectives (different angles/common goals).

Open the lines of communication.

The major objectives are to:

Define expectations of new/existing policy (Government defines/Industry provides feedback and implements).

Share resources (educational materials, problem solving, lessons learned, technological advances).

Crystal City Security Awareness Group

This group consists of security professionals concerned with the protection of employees and assets. The group's primary goal is to provide a safe environment for the conduct of normal business operations through awareness and the pooling of

collective resources. The overriding concern is to educate, share and disseminate information on security and safety. It meets monthly to exchange information and receive training in areas of mutual concern. The membership represents private industry, government agencies, and security organizations. Some of the topics the group has addressed include: Industrial Security Issues, Landlord/Tenant Concerns, the Availability of Perimeter and Equipment Security Products, FBI Counterintelligence Briefings, Emergency Planning, Traffic Engineering, Substance Abuse in the Office Place, Bomb Threat Policies and Procedures, Rape Prevention, Monthly Crime Statistics for the Crystal City Area, and Computer Security.

Arlington Security Group (ASG)

The purpose of the ASG is to provide contractor-organized security education and training to the security personnel of those organizations that fall under the cognizance of the Arlington Field Office. Meetings are held on the last Thursday of each month and events for the group are planned by its steering committee. The group has sponsored a tour of the FBI, a one day STU III/COMSEC seminar and training on how to accomplish security education on a shoestring budget. It plans to sponsor seminars on managing stress and conducting administrative inquiries. A newsletter announcing upcoming events, dates of steering group meetings, job opportunities, security tips and other items of security related interest is published monthly. The impetus for this group comes from the contractors who participate in it. The security advice and assistance is provided by DIS. Representatives from User Agencies and the local police office have attended past meetings.

The I-270 Corridor Security User Group

This group was formed in October 1990 with the primary objective of allowing local security professionals the opportunity to discuss and share information on a myriad of industrial security issues. It meets bimonthly at alternating contractor locations under the cognizance of the local DIS industrial security field office (S15WP). The group is comprised of approximately 50 government and contractor representatives with two co-chairs, the local field office chief and a contractor.

Besides sharing information pertinent to industrial security policy, the group regularly obtains speakers to present informal discussion of relevant topics. They have had speakers from the National Security Agency, the Defense Industrial Security Review Board, Underwriters Laboratories, the Interagency Operations Security Support Staff, the FBI, DIS Headquarters, and Senior Managers in Industry. The group sponsored a one-day refresher seminar for security officers which highlighted participation from both contractor and government personnel.

More recently, the group has begun to focus on existing procedures in an attempt to improve them. A committee has been formed to address the requirements of the adverse information reporting procedure. Their objective is to develop an instrument which security officers can use to maximize management's participation and support for this process. The co-chairs of this group welcome any suggestions or comments which may help.

Ms. Scardina is an instructor at the DoD Security Institute

Industrial Security Awareness Councils — ISACs

San Diego
POC: Mr. Bob Harman
c/o FBI
880 Front Street, Suite 6S13
San Diego, CA 92188
(619) 557-4389

Greater Los Angeles
POC: Ms. Linda Kimbler
Defense Investigative Service (V5300)
3605 Long Beach Blvd., Suite 405
Long Beach, CA 90807-4013
(310) 595-7666

Vandenberg
Chair: Mr. Walt Tomlinson
P.O. Box 5791
Vandenberg AFB, CA 93437-5791
(805) 734-8282 ext. 5-0766

San Francisco Bay Area
POC: Ms. Cam Donald
GTE Government Systems
100 Ferguson Drive
P.O. Box 7188
Mountain View, CA 94039
(415) 966-4108

North Bay
POC: Ms. Sandra Ryan
Security Manager
Optical Coating Laboratory, Inc.
2789 Northpoint Parkway
Santa Rosa, CA 95407-7397
(707) 525-7548

East Bay
POC: Mr. John Whitecotton
Defense Investigative Service
Industrial Security Resident Office
620 Central Avenue
Building 2G, Room 113
Alameda, CA 94501-3801
(510) 522-2008

Central Valley
POC: Mr. Ray Miller
Aerojet Propulsion Division
P.O. Box 13222 D5630/B2006
Sacramento, CA 95813-6000
(916) 355-1000 ext. 3412

Silver State
POC: Ms. Melanie Scheid-Myers
Loral Aerospace Services
P.O. Box 1950
Fallon, NV 89407-1950
(702) 423-3841

Phoenix
Co-Chair: Mr. Ed Hyland
Senior Industrial Security Representative
Defense Investigative Service (S42PX)
201 East Indianola, Suite 360
Phoenix, AZ 85012-2055
(602) 640-2448

Co-Chair: Mr. Gregory Meagher
Security Manager
Motorola, Inc.,
Government and Electronics Group
8201 E. McDowell Road
P.O. Box 1417
Scottsdale, AZ 85252

Salt Lake City
POC: Mr. Joe Cotton
Paramax Systems Corporation
640 North 2200 West
Salt Lake City, UT 84116
(801) 594-5615

Southwest
POC: Ms. Betty Kreeger
Cortez III Service Corporation
115 S. Florida
P.O. Box 2029
Alamogordo, NM 88310
(505) 437-5201

POC: Mr. Art Marquez
STEWS-SD-S
White Sands Missile Range, NM 88002-5041
(505) 678-4502

New Mexico
POC: Mr. Dave Coulie
Honeywell, Inc.
Avionic Systems Division
9201 San Mateo Blvd. N.E.
Albuquerque, NM 87113-2227
(505) 828-5430

Rocky Mountain Region
POC: Mr. Mike MacDonald
Defense Investigative Service (S42DR)
P.O. Box 8718
Denver, CO 80201-8718
(303) 844-5233

North Texas Joint
POC: Mr. Jim Bass
General Dynamics Corporation
P.O. Box 748
Ft. Worth, TX 76101
(817) 777-4535

Minnesota
Chair: Mr. Jay Dombrowski
Northwest Airlines, Inc.
2700 Lone Oak Parkway
Eagan, MN 55121
(612) 727-7043

POC: Donna MacHolda
Industrial Security Representative
Defense Investigative Service
P.O. Box 17159, Nokomis Station
Minneapolis, MN 55417-7128
(612) 725-8053

Chicago
POC: Ms. Catherine Allen
Recon Optical, Inc.
550 West Northwest Highway
Barrington, IL 60010
(708) 381-2400

Huntsville
Co-Chair: Ms. Sherry Grasson
General Research Corporation
635 Discovery Drive
Huntsville, AL 35806
(205) 922-1941

Co-Chair: Mr. John Murphy
USA Strategic Defense Command
P.O. Box 1500
Huntsville, AL 35807-3801
(205) 955-1726

South Florida
Acting Chair: Jim Radovic
United Technologies Pratt & Whitney
P.O. Box 109600
West Palm Beach, FL 33410-9600
(407) 796-2312

POC: Mr. Kirk Paulsen
Defense Investigative Service (S41PB)
1818 S. Australian Avenue, Suite 251
West Palm Beach, FL 33409-6447
(407) 684-9384

Florida East Coast
POC: Mr. Rick D'Oria
Defense Investigative Service (S41ME)
1333 Gateway Drive, Suite 1009
Melbourne, FL 32901-2629
(407) 951-4412

Chair: Ms. Harriet Zbiegien
Rockwell International Corporation
Space Systems Division
8600 Astronaut Blvd.
Cape Canaveral, FL 32920
(407) 799-6886

Atlanta
POC: Ms. Kathy Pritchett
Defense Investigative Service (V4100)
2300 Lake Park Drive, Suite 250
Smyrna, GA 30080-7606
(404) 432-0826

Chair: Mr. Albert Schwarz
AEL Defense Corporation
Cross Systems Division
1355 Bluegrass Lakes Parkway
Alpharetta, GA 30201-7700
(404) 475-3633

Dulles
POC: Mr. Bob Cross
Defense Investigative Service (S15DS)
12355 Sunrise Valley Drive, Suite 170
Reston, VA 22091-3415
(703) 487-8096

The I-66 Corridor
POC: Mr. Mike Yovino
EG&G Washington Analytical Services Center, Inc.
8809 Sudley Road
Manassas, VA 22110
(703) 631-2670

POC: Mr. Mark Allen
Defense Investigative Service (S15DS)
12355 Sunrise Valley Drive, Suite 170
Reston, VA 22091-3415
(703) 487-8096

Tyson's Area
POC: Mr. Bob Cross
Defense Investigative Service (S15DS)
12355 Sunrise Valley Drive, Suite 170
Reston, VA 22091-3415
(703) 487-8096

JIGSAG
Chair: Ms. Peggi Parks
HDS, Inc.
12310 Pinecrest Road
Reston, VA 22091
(703) 620-6200

Northern Virginia
POC: Mr. Dan Wright
The MITRE Corporation
7525 Colshire Drive
McLean, VA 22102
(703) 883-6650

POC: Ms.Dorothy Borsi
Field Office Chief
Defense Investigative Service (S15AX)
25 S. Quaker Lane
Alexandria, VA 22314
(703) 617-0051

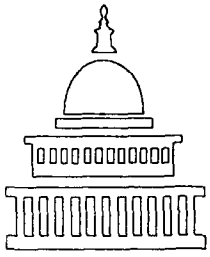
Crystal City
POC: Ms. Linda Mitchell
Rockwell International
1745 Jefferson Davis Highway
Arlington, VA 22202
(703) 553-6867

Arlington
POC: Ms. Carol Caul/Ms. Regina Hellmann
Industrial Security Representatives
Defense Investigative Service (S15AR)
1815 N. Fort Myer Drive
Arlington, VA 22209
(703) 696-5308

I-270 Corridor
Co-Chair: Mr. Greg Pannoni
Field Office Chief
Defense Investigative Service (S15WP)
510 Wheaton Plaza South
Wheaton, MD 20902-2538
(301) 427-5587

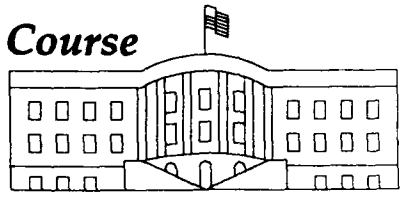
Co-Chair: Ms. Kay Mehner
IBM Federal Systems Company
800 N. Frederick Avenue
Gaithersburg, MD 20879

If you are part of an ISAC or any group that regularly meets to discuss security issues, let us know who you are and more importantly, let others know who you are. Some of the "more established" councils out there are ready to help you. So let's work together to maintain this network. All input for this network should be submitted to the DoDSI, 8000 Jefferson Davis Highway, Richmond, VA 23297-5091 or faxed to (804) 279-5239, Attention: Security Education & Awareness Team — ISAC Network.



The Industrial Security Management Course

will be offered in the
Washington, DC Area
September 27 through October 1, 1993



The Industrial Security Management Course provides four and a half days of training covering the requirements of the Defense Industrial Security Program (DISP). Specific topics include the Administrative Structure of the DISP, Facility and Personnel Security Clearances. Visitor Control, Safeguarding Classified Information, Classification Management, Security Education, Security Violations and Compromises. Special guest speakers include Special Agents from the Federal Bureau of Investigations (FBI) who speak from personal experience about the threats to US technology and information from foreign countries and companies. Regional DIS personnel also participate in this course. The course will be held in the auditorium at Software Productivity Consortium, 2214 Rock Hill Road, Herndon, VA.

This is the course required for some Facility Security Officers by paragraph 3-101 b. of the Industrial Security Manual for Safeguarding Classified Information.

To enroll, mail this page to:

Defense Investigative Service
Director of Industrial Security
Attn: (S1511)
2461 Eisenhower Avenue
Alexandria, VA 22331-1000
(703) 325-9395

Title of Course: *Industrial Security Management Course*

Location: Herndon, VA **Course Dates:** Sept. 27 - Oct. 1, '93

Your Name: Mr. Mrs. Ms._____
(circle one) (Last), (First) (MI)

Job Title: _____ **Military or GS Grade:** _____

Business Address:

_____ **Supervisor:** _____

_____ **Supervisor's Phone:**(___)____-_____

_____ **Your Phone:** (___) ____-_____

How long have you been an FSO? _____

Have you completed these independent study courses?

Essentials of Industrial Security Management _____

Protecting Secret and Confidential Documents _____

CAGE Code Number: _____

The Security Program Improvement Network (SPIN)

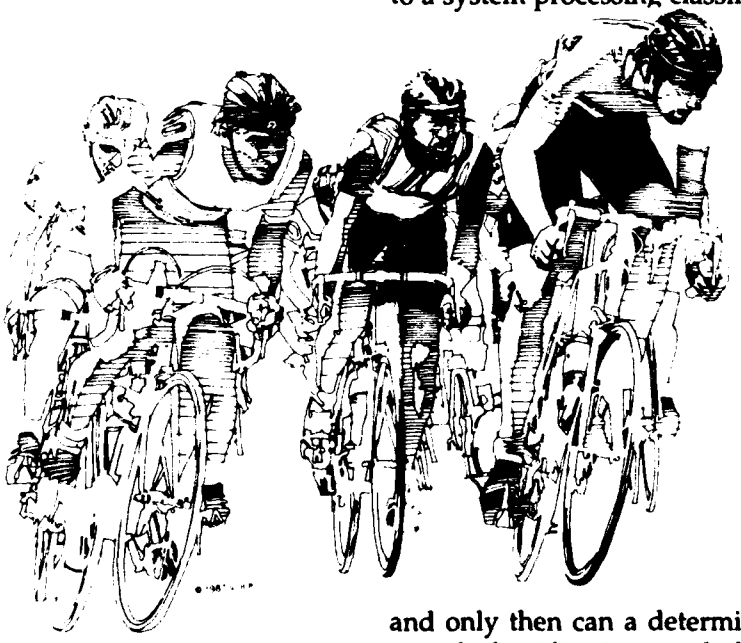
by Carl Roper

Since the SPIN program concept was instituted and word passed to you through the Security Awareness Bulletin, items of interest have been received. The following are some SPIN related efforts that are of interest and can be used by all readers.

Classified AIS

Paramax (a Unisys company) prepares a Security Awareness Bulletin on a variety of subject areas for its employees. The following is from Elaine Townsend, Facility Security Officer, Paoli, PA.

The System Security Supervisor for your area is responsible for ensuring that the AIS is operated and maintained in compliance with government mandated policies and practices. This can only be accomplished with your ongoing cooperation. Consult the System Security Supervisor before changing or introducing new hardware, software or firmware into the approved AIS.



Protection of Software

Before **any** software is *initially* introduced into the AIS , it must be reviewed and approved for use by the System Security Supervisor to preclude the introduction of malicious logic into the system which may adversely affect the security of future classified processing.

Media storing system software must be marked and safeguarded to the highest level of intended classified processing. Additionally, if the software contains security related-functions, i.e., declassification, access control, auditing, etc., it must be validated to confirm that every security related feature is fully functional before it can be used during a classified processing period. Other unclassified software may be introduced into a classified processing period only from a source which is "write protected." Software used during classified a processing period, without write protection, must be classified and safeguarded at the highest level of information processed.

SPIN NOTE: Any time software is introduced to a system processing classified, you must assume that some data transfer will take place, intentionally or unintentionally. As such, the software—and any item[s] of information extracted, need to be marked and protected at the highest level for which the system is authorized to process. For any printouts, once it has been **completely reviewed** by an individual with subject matter knowledge of the information, then and only then can a determination be made of its actual classification, and the printout properly marked!

Heading Off Computer Security Deficiencies

Deficiencies have been cited by DIS inspectors for the use of unapproved computer systems to process classified information. Recommended countermeasures to deter the unauthorized use of AIS systems by employees include:

- Use only those systems approved by the organizational/AIS security office to process classified information.

- Ensure there are a sufficient number of approved systems available to meet the needs of your workforce and that they are reasonably accessible to the users.

- Perhaps most importantly, educate all your PC users in the proper security procedures to be followed, making sure the employees know where the approved systems are located and whom to contact should they need a need existing system approved to process classified information.

If you need assistance with AIS security procedures, contact the security office or your AIS system administrator.

SPIN NOTE: These are some good words to heed and pass on. All computer operators, whether new or experienced, should be aware of the above. Rushing to get a project done or meeting a deadline is no reason to circumvent the approved system. A few minutes of discussion, explaining the situation, and a little coordination with the AIS administrator, can ensure the job gets done, but is done properly and within the framework of the DOD requirements.

Computer Password Selection

The most frequently used computer password is "password," according to Allan Brill, Kroll Associates. The screen prompts with "enter password" and, sure enough, many users will key in "password."

SPIN NOTE: Anyone in the computer field realizes the benefit of using a random type selection for any password. Anywhere from five to 15 characters, be they alpha, numeric, or an alphanumeric combination, provides the greatest protection against unauthorized access to a computer system. The AIS security manager could have the user ID and/or password computer generated in a random mode, which would ensure against users determining their own and using commonly detectable access codes.

Care and Maintenance of Your PC Floppy Disks

The National Computer Security Center has this advice for the proper care of those floppy disks. With the PC advent, we now keep thousands of pages of information on floppy disks within our offices. Just like a paper product, some basic procedures need to be considered to ensure your floppies will be useable when you need them.

- Keep disks in their protective jackets when not in the drive unit.
- Keep the disks stored upright in their boxes.
- Keep the disks clear of eraser crumbs, dust, and smoke particles.
- Use a felt tip pen when writing on the disk label. Pencil or ball point pressure can destroy floppy precision.
- Make a back up copy of the important disks and store them separately from the originals.
- Don't touch the disk surface. It's easily contaminated, so something as minor as a fingerprint can cause error. On a dry day, your finger could have enough electrostatic charge to damage the data permanently.
- Don't use alcohol, thinners, or Freon to clean the disk. Chemical fumes can endanger the magnetic coating, so don't expose it to solvents like nail polish or duplicating machine fluids.
- Don't expose the disk to magnetic or magnetized objects. Data can be destroyed, scrambled, or wiped out completely. A color television, CRT, electric motor, or other devices can destroy data integrity. Screwdrivers, paper clips, car keys, or any metal object may also be magnetized.
- Don't put a telephone on top of a disk, the disk drive, or a box of disks. Once ring can cause damage.
- Don't expose the disk to home power supply units.
- Don't bend, fold, or use rubber bands or paper clips in the disk. Any warping can lead to mistracking.
- Don't rest heavy objects on the disk. It can cause a crimp that would lead to mistracking.
- Protect your floppy disk at least as well as you would the data on it.

SPIN NOTE: These are some good words to read and heed. With more and more data being PC processed, we have an inherent duty to protect that data as best we can. By following the above

measures, we can ensure our data will be protected and ready for use when we need it.

The Cost of Keeping Classified in Your Files

It costs money to maintain classified material at any activity. McDonnell Douglas has taken some good steps to reduce their inventory due to costs, as passed to us by Bill Giese, Group Manager for Security at McDonnell Douglas, St. Louis, Missouri.

An industry survey associated with the NISP effort, and a recent Council of Defense and Space Industry Associations (CODSIA) case, have produced some significant results on the cost of storage, inventory, accountability and retention of accountable classified material has produced some significant results.

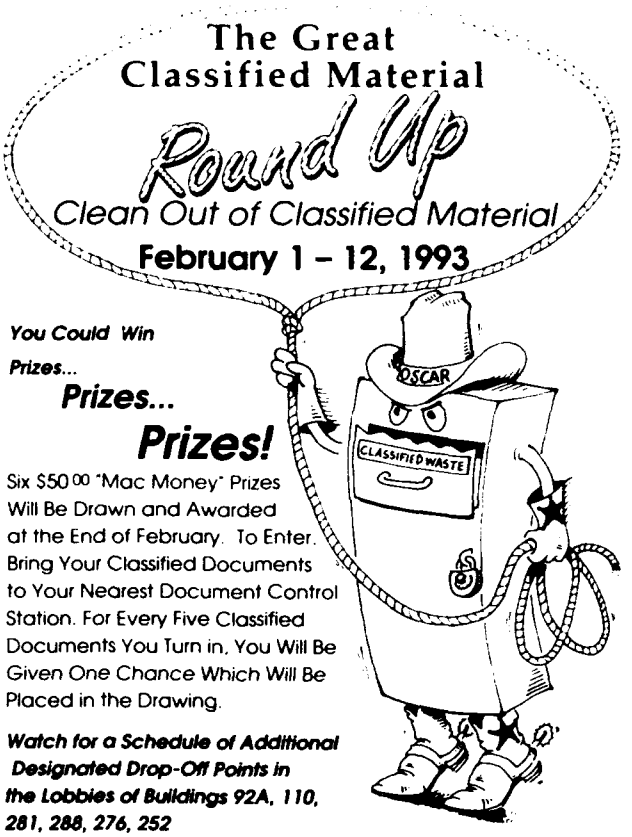
Did you know it takes about 98 minutes per year (or approximately $75.00 a document) to maintain each item of accountable (Secret and Top Secret) classified material. Because of this, a major push toward reducing accountable documents can demonstrate significant savings.

The Security Department promoted a review and cleanout of material in February of this year. Flyers, with a cartoon figure, a buzzword ["Roundup"] and some gift certificates as prizes, proved most effective. The two main points of the program were:

- Clean out the classified materials that are no longer needed or required.
- For every five documents turned in for destruction, the individual got a chance for a $50.00 gift certificate [total of $300.00 for the effort].

The results: 2,712 accountable documents turned in for destruction. At $75.00 per document, this was an immediate $203,400 savings for McDonnell Douglas.

SPIN NOTE: McDonnell Douglas used an incentive to motivate people. The document cleanout program cost was negligible when compared to the thousands of dollars saved for the company. A tip like this from private industry can also help government security officers motivate people to clean out those extraneous documents that are no longer needed. Put on your thinking cap, do a little planning, and get some good results!



Employee Safety & Awareness

Employee safety and security awareness tips can be generated and passed on to your employees. Remember, security can be effective and also show a personal concern for employees both on and off the job. McDonnell Douglas, again, looks to the employees' welfare all the time. The following tip from one of McDonnell Douglas' 1993 newsletters identifies a concern of personal safety and what the individual can do to reduce a potential threat:

Safe/Secure ATM Transactions

Automatic Teller Machines (ATMs) are convenient to use but caution should be taken when making transitions. The Security Investigations department has provided the following safety tips for using an ATM

1. Avoid using the machines late at night. Most ATM crimes occur after regular banking hours.

2. Use only well-lit secure ATM locations, preferably where there is a guard on duty. The area should be busy, not secluded or deserted. Check for people loitering nearby or across the street. If the location does not seem safe, got to a more secure ATM.

3. Be sure to sign off the machine when you have finished your transaction. Criminals often try to break into accounts that are still open on the ATM screen and withdraw cash.

4. Make sure to take your card with you when you leave the ATM. Never give your card to anyone else to use. It's a common ruse among scam artists to request the use of a stranger's card - they'll claim they simply want to gain access to the computer so they can do their own banking, but what they really want is access to *your* bank account.

SPIN NOTE: Advice and tips such as above are timely and demonstrate a concern by the security office for the well-being of employees. Some other ATM tips you may wish to include are:

- Withdraw only the cash you actually need. Don't withdraw "extra" cash just in case you may need more.
- If possible, park your vehicle close to the ATM so you don't have far to walk once you have completed your transaction.
- **Never** write the PIN number on your ATM card, much less keep it in the same place. The best method is to memorize the PIN number.
- If you are in the process of using the ATM and a suspicious person approaches, log off the machine, remove your card putting it away and move away from the ATM to the safety of your car. (You can always come back, if your suspicions are unfounded, but it's better to be safe than sorry.)

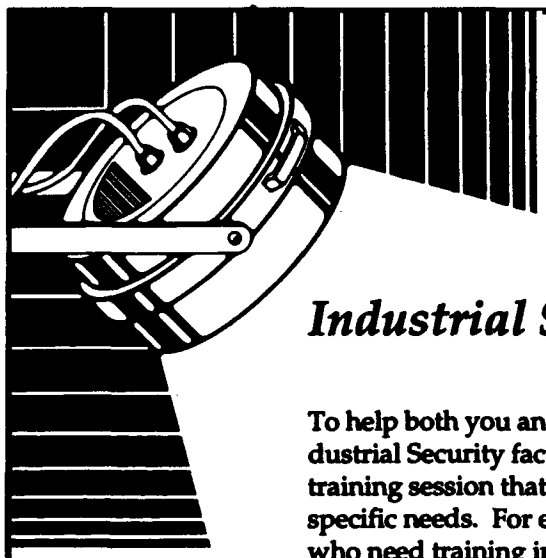
The above are but a sampling of SPIN items available through the DOD and contractor field. Certainly your command, organization, or local activity has come up with ideas that can help others through the SPIN network. Like the above items, send them in and we'll share them with the world, so everyone can benefit.

All ideas are welcome. If it's worth considering, it's worth letting others know so that their security program can also improve.

Forward your thoughts, ideas, or other security-related items to:

DoD Security Institute
Attn: SPIN Coordinator
c/o DGSC
8000 Jefferson Davis Hwy
Richmond, VA 23297-5091

Mr. Roper is the SPIN coordinator. He is also an instructor with the Information Security Team at the DoD Security Institute.



Industrial Security — Customized

To help both you and the already overworked Industrial Security Rep, the Industrial Security faculty at DoDSI will work with you to create a one- to two-day training session that covers industrial security subjects *you* can tailor to your specific needs. For example, do you have numerous Document Control personnel who need training in accountability, reproduction, destruction? We can help. You pick the site; no cost other than travel, food, and lodging for one or two instructors. For government and industry.

For more details about this offer, please call Wayne Lund on (804) 279-3939.

New reduced price . . .

Is Your PC Data Safe?

Date: 1992 Length: 21 min. Cost: ~~$325.00~~ $79.00 if prepaid; $99.00 with purchase order

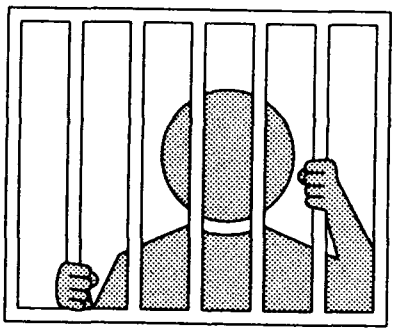
Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Summary: This computer security training program for government contractors comes with a 21-minute video, instructor's manual, and student guide materials. Video shows the importance of following the guidelines in Section 8 of the Industrial Security Manual, and your SPP. Dramatization tells the story of a new company president with a poor security posture and the tips he receives from his ghostly colleague. Video is closed captioned for hearing impaired. Produced by Pro Star International. Program also comes in a second version: Protecting trade secrets and proprietary information.

Video . . .

an 18-minute video based on interviews of convicted espionage felons, designed to motivate employees and military personnel to support personnel security programs through timely intervention.

You Can Make a Difference



First in a series of six videos — each of which will focus on a different aspect of espionage, and what can be learned, from the point of view of the offender.

You Can Make a Difference is marked For Official Use Only. It is not releasable for public viewing or to the media. Now being distributed to Federal agencies and departments, cleared contractors may obtain a copy by written request through FilmComm Inc.

To government contractors: Because this is an FOUO product, we ask you to certify in your order that, when received, "This video product will be used only for the training and education of employees or personnel in support of a federal government security program."

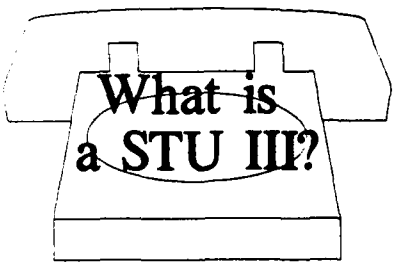
Prepaid cost is $21.50 plus $2.50 for shipping for 1/2". *Invoiced* requests are $23.50 and $2.50 for shipping. } *(For 3/4" add $10.00.)*

For additional ordering details, please call FilmComm.

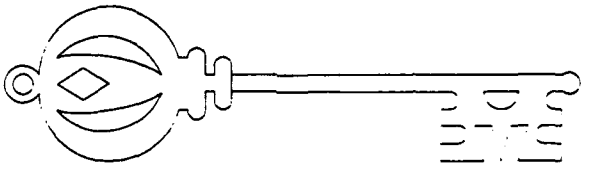
To order:
FilmComm Inc.
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

This video has been produced by the Department of Defense Security Institute in cooperation with the National Advisory group for Security Countermeasures and Project Slammer.

How do I get a STU III?
How do I use it?



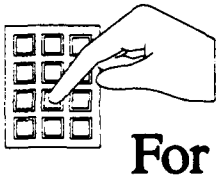
What is "Seed Key"?



What are the storage requirements for *my STU III equipment and key?*

What do I need to know about COMSEC accounting procedures?

What types of STU III products are available?



For more information about hosting this one-day course for security professionals in your area please call Wayne Lund at the DoD Security Institute, (804) 279-3939.

Introduction to the STU-III

This course gives the new STU-III user basic guidance in how to use the STU-III and what Security responsibilities they have. It is an ideal course for COMSEC Custodians of STU-III Only COMSEC Accounts (SOCA's) and for people who are not COMSEC Custodians but have some security responsibility for STU-III units at their work site.

Course Dates in Richmond, VA

October 14, 1993	February 17, 1994	May 26, 1994
October 28, 1993	March 10, 1994	August 11, 1994
November 18, 1993	March 31, 1994	
December 16, 1993	April 21, 1994	

[Note: This course is not intended to be a substitute for the COMSEC Custodian Course (CS-140) offered by NSA.]

Complete Two Classes in Two Days!

This Course Schedule is coordinated to allow you to attend *Classification Management in the DISP* one day followed by *Introduction to the STU-III*. You may complete both courses with just one trip to Richmond!

Other dates and locations may be scheduled upon request. To host this course at your location, contact Wayne Lund at (804) 279-3939.

To enroll, mail this page to:

DoD Security Institute
Attn: Registrar
8000 Jefferson Davis Highway
Richmond, VA 23297-5091

Title of Course: *Introduction to the STU-III*

Location: Richmond, VA **Course Dates:** _____

Your Name: Mr. Mrs. Ms. _____
(circle one) (Last), (First) (MI)

Job Title: _____ **Military or GS Grade:** _____

Social Security Number: ___-___-___ **Date of Birth:** _____

Business Address:

_____ **Supervisor:** _____

_____ **Supervisor's Phone:** (___)___-____

_____ **Your Phone:** (___)___-____

Classification Management in the DISP

This class provides current up to date information regarding the preparation of the DD Form 254. Proper use of markings on classified documents can also be discussed. The class is designed for Contractor employees, User Agency personnel and others in government and industry who are involved in preparing this form or giving classification guidance.

Course Dates in Richmond, VA

October 13, 1993	February 16, 1994	May 25, 1994
December 15, 1993	March 9, 1994	

Complete Two Classes in Two Days!

This Course Schedule is coordinated to allow you to attend *Classification Management in the DISP* one day followed by *Introduction to the STU-III*. You may complete both courses with just one trip to Richmond!

Other dates and locations may be scheduled upon request. To host this course at your location, contact Floyd Dunstan at (804) 279-5307.

To enroll, mail this page to:

DoD Security Institute
Attn: Registrar
8000 Jefferson Davis Highway
Richmond, VA 23297-5091

Title of Course: *Classification Management in the DISP*

Location: Richmond, VA **Course Dates:** _____

Your Name: Mr, Mrs, Ms, _____
(circle one) (Last), (First) (MI)

Job Title: _____ **Military or GS Grade:** _____

Social Security Number: ___-___-___ **Date of Birth:** _____

Business Address:

_____ **Supervisor:** _____

_____ **Supervisor's Phone:** (___)___-____

_____ **Your Phone:** (___) ___-_____

announcing . . .

AIS Security Procedures For Industry Course (AIS-I)

The 3½ day AIS-I provides contractors with practical experience in reviewing AIS Standard Practice Procedures (AIS SPPs) and conducting AIS Self-Inspections. The Defense Industrial Security Program requirements for processing classified information in data processing and office automation systems are explained, together with supporting rationale.

Topical areas include: discussion of AIS security procedures and guidelines; and applicable AIS SPP outlines prepared and distributed by DIS activities. Using guidance provided during the course, students will review an AIS SPP for a microcomputer system and inspect the system in accordance with Chapter 8 requirements of the Industrial Security Manual (ISM).

Next field extention course held in Washington, DC
September 21-24, 1993

The course will be held at the DoD Security Institute on
November 15-19, 1993.

There is no tuition for the course and a security clearance is not required. To be eligible for attendance, students must prepare or have oversight responsibility of AIS Approval and AIS SPPs. Upon acceptance to the course, students must complete a series of Work-Ahead-Modules (WAMs) which will be issued to them approximately one month prior to the commencement of the course. Class size is limited, so registration is accomplished on a first come, first served basis.

For course details, call the AIS Division, (804) 279-5309 or 279-4187.

Mail this page to: Attn: Registrar
DoD Security Institute,
c/o DGSC
Richmond, VA 23297-5091

Your Name Mr./Mrs./Ms._____

Position _____

SSN _____

Company Name _____

Address _____

_____

_____

Telephone _____

Supervisor _____

Course Title AIS Security Procedures for Industry

Course Dates _____

Training Resources for the ASPP

A series of exportable training modules have been developed to provide additional information on acquisition systems protection.

- Introduction to Acquisition Systems Protection: A 90-minute course of instruction designed to orient personnel on the basics of acquisition systems management and introduce the fundamentals of the protection program.

- Acquisition Systems Protection (Advanced): A 4-hour lesson designed for practitioners developing program protection plans.

- Acquisition Systems Protection for Acquisition Professionals: A 90-minute lesson focusing on the enabling disciplines for protection planning such as security countermeasures, counterintelligence support, operations security and intelligence support.

Projected training tools include video tapes and correspondence courses.

For more information on these products contact your organization's protection specialist or security manager. Additional information is also available from the Acquisition Systems Protection Office or the Defense Security Institute, ATTN: Cynthia Kloss, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091.

Don't Keep it a SECRET, spread the word about the Defense Security Institute's

INFORMATION SECURITY ORIENTATION COURSE

Who is the course designed to serve?

Government employees who are:

- Part-time security managers and assistant security managers
- People who need an overview of the information security program
- People who have responsibilities pertaining to classified information
- People who regularly handle classified information
- Document control personnel
- TSCOs and alternates

How long is the course?

- Three days

Where is it held?

- Courses are given at the sponsor's location of choice. We are looking for sponsors for FY 94.

How much does it cost?

- Per diem and travel costs for two instructors.

How can I find out more?

- **Call Course Manager Cheryl Cross at DoDSI, DSN 695-4390, COMM (804) 279-4390. fax: DSN 695-5239, (804) 279-5239**

What is included in the course?

- The classification process
  - Who can originally/derivatively classify
  - Original classification process
  - Derivative classification process
  - Applying theory with practical exercises
- Marking information
  - Markings common to all classified and unclassified sensitive documents
  - Applying theory with practical exercises
- Accountability and control systems
  - TS accountability procedures
  - Secret/Confidential procedures
  - Two-person integrity
  - Classified reproduction procedures
- Custodial responsibilities
  - Security Standard Forms
  - Mailroom
  - End of the day security check
  - Exit/entrance inspection program
  - Courier authorization card
- Safes and locks
  - GSA containers
  - Other types of containers
  - Authorized locks
- Transmission/transportation
  - Transporting
  - Packaging
  - Handcarrying
- Disposal/destruction
  - Who can?
  - When to?
  - Methods
  - Procedures
  - Precautions
- Violations/compromises

Security Awareness Publications Available From The Institute

Publications are free. Just send this form with mailing label **to:**

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314 or DSN 695-5314

(TAS) Training Aids for Security Education. June 1992. Catalog of audiovisual and printed material of interest to security educators. Instructions for ordering. . . . . ___

(REC) Recent Espionage Cases: Summaries and Sources. August 1992. Seventy-eight cases, 1975 through 1991. "Thumb-nail" summaries and open-source citations. . . . . ___

(FIT) The Foreign Intelligence Threat to U.S. Defense Industry. By Defense Security Institute staff. January 1991. . . . . ___

(CUT) Control of Unclassified Technical Data with Military or Space Application, May 1985. DoD 5230.25-PH. 20-page booklet prepared by the Office of Secretary of Defense explaining the DoD program to limit public disclosure of export-controlled technical data and the special markings for technical documents. . . . . ___

DELIVER! Easy-to-follow pamphlet on how to transmit and transport your classified materials. . . ___

Terminator VIII Requirements for destruction of classified materials. Contains questions and answers for some common problems and also detailed information on various destruction methods. . . . . ___

STU-III Handbook for Industry . . . . . ___

Survival Handbook, the basic security procedures necessary for keeping you out of trouble . . . ___

Security Awareness Bulletin. Back issues available from the Institute:

(1-90) Oct 89	Foreign Travel. FOR OFFICIAL USE ONLY.	___
(2-90) Jan 90	The Case of Randy Miles Jeffries	___
(3-90) Apr 90	Beyond Compliance – Achieving Excellence in Industrial Security	___
(1-91) Jan 91	Regional Cooperation for Security Education	___
(2-91) Sep 91	AIS Security	___
(1-92) Oct 91	Economic Espionage	___
(2-92) Feb 92	Self-Inspection Handbook	___
(3-92) Mar 92	OPSEC	___
(1-93) Apr 93	Acquisition Systems Protection	___

*U.S. Government Printing Office: 1993 — 356-432/90079